DCI Draft

EVALUATING THE PROTECTION OF SENSITIVE INFORMATION AT OFFICIAL UNITED STATES FACILITIES ABROAD (U)

1. The security of sensitive information at official US facilities abroad is vital to the effectiveness of national security activities undertaken at these facilities. Intelligence information shows that hostile intelligence services have gained access to sensitive information at official US facilities abroad through technical penetration or other means which circumvent our protective security measures. A key element of providing necessary security to official US facilities abroad is an ability to evaluate threats to and vulnerabilities of our sensitive information. (C)

NSA review completed

State Dept. review completed

State Rewrite

EVALUATING THE PROTECTION OF SENSITIVE INFORMATION AT OFFICIAL UNITED STATES DIPLOMATIC AND CONSULAR FACILITIES ABROAD (U)

1. The security of sensitive information at official US diplomatic and consular facilities abroad is vital to the effectiveness of national security activities undertaken at these facilities. Intelligence information shows that hostile intelligence services have gained access to sensitive information at official US diplomatic and consular facilities abroad through technical penetration or other means which circumvent our protective security measures. A key element of providing necessary security at official US facilities abroad is an ability to evaluate threats to and vulnerabilities of our sensitive information and to make timely decisions on methods to eliminate or exploit our knowledge of hostile penetrations.

NSC review completed

NSA Comments

2. This NSDD sets forth policy on a comprehensive security evaluation program to protect sensitive information at certain US facilities abroad. (C)

Policy

3. The US shall maintain and use at official facilities abroad technically competent, properly equipped and continuing capabilities to detect and assess threats and vulnerabilities to the security of sensitive information at these facilities. The Secretary of State has primary responsibility for the security of US diplomatic and consular facilities abroad. No technical survey or evaluation activity, overt or covert, will take

2. This NSDD sets forth policy on a comprehensive security evaluation program to protect sensitive information at certain US facilities abroad. The sophistication of the technical penetration threat requires a strengthening and refurbishment of our national capabilities through through increased intelligence community coordination, improved expertise, and aggressive and farsighted research and development.

3. The Secretary of State has primary responsibility for the security of our diplomatic and consular facilities abroad. The Secretary of State shall maintain and use at official diplomatic and consular facilities abroad technically competent, properly equipped and continuing capabilities to detect and assess threats and vulnerabilities to the security of sensitive information at these facilities. No technical survey activity, overt or covert, will

place in a diplomatic or consular facility abroad without his explicit approval. (C)	take place in a diplomatic or consular facility abroad without his explicit approval.	
Implementation		
4. I direct that the government's capabilities for detecting and assessing hostile threats to the security of official facilities abroad, and evaluating the effectiveness of existing and planned US security counter-measures, be maintained, improved, developed or established to support this policy. (C)		
5. In support of the Secretary of State and under the direction of the Director of Central Intelligence, the National Security Agency will: (U)	4. In support of the Secretary of State the DCI will form an inter-agency group of offensive and defensive technical penetration experts to conduct surveys of overseas US facilities. Staffing of these interagency evaluation teams will be determined by the DCI with the approval of the Secretary of State and may be drawn from NSA, DOS, FBI or CIA. The focus of these special surveys will be on those	5. "In support of the Secretary of State and under the direction of the Director of Central Intelligence....." RATIONALE: The Secretary of State has been left out of this draft. Previous draft wording should be adopted.
a. Assemble and deploy teams of experts in both the offensive and defensive aspects of technical penetration drawn from various departments and agencies of the government, including the National Security		

Agency, the Department of State, the Federal Bureau of Investigation and the Central Intelligence Agency. These teams will conduct evaluations to detect and assess electronic penetration threats and vulnerabilities and recommend effective countermeasures. (S)

US facilities in the USSR, bloc and other locations where hostile penetration efforts are assessed to be highly likely. Such surveys are not a substitute for standard technical security procedures and other security inspections that are routinely conducted under the authority of department and agency heads.

The joint survey teams may be requested at any time by the Secretary of State or a participating member organization. The Secretary of State must approve all ensuing missions.

The survey teams will be constituted of the best talent available and charged with performing the following functions:

a. Conduct evaluations to detect and assess the technical penetration threats and vulnerabilities and to recommend timely and effective countermeasures.

b. In coordination with the Department of State, Central Intelligence Agency, Federal Bureau of Investigation and other appropriate departments or agencies of the government, ensure that knowledge of a specific evaluation is controlled to the maximum extent necessary to enable an evaluation to proceed from conception through institution of final recommendations without the knowledge of hostile intelligence services. (S)	b. Ensure a strict operational security posture that protects teams from alerting hostile intelligence services to planned visits, suspected targets, and to sensitive search and detection techniques employed.	b. "In coordination with the Secretary of State, Deputy Director of Central Intelligence, Director of the Federal Bureau of Investigation, and other appropriate senior officials of the government, ..." RATIONALE: Supports in a more clear way the sensitivity of the operation and the need to control knowledge of the operation.
c. Report to the Assistant to the President for National Security Affairs, through the Director of Central Intelligence and the Secretary of State, on evaluations and activities of the interdepartmental evaluation teams. Heads of departments and agencies affected by the evaluations or activities of the teams will receive such reports as may affect their interests. (S)	c. Prepare a report of findings for the Assistant to the President for National Security Affairs, via the Secretary of State and the Director of the Central Intelligence.	c. "Report to the National Security Council via the Systems Security Steering Group; Director of Central Intelligence....."; RATIONALE: The Director of NSA believes the Steering Group is the appropriate group to be involved. This wording also adds the Secretary of State in the reporting mechanism.

d. Share with other departments and agencies of the Intelligence Community and the Department of State information on methods of operation that are or may be used by hostile intelligence services, and on countermeasures against such penetration methods. (C)

e. Provide instructors and up-to-date-information to the Interagency Training Center to ensure that technical surveillance countermeasures specialists are abreast of the state of the art of offensive technical penetration, consistent with operational security considerations. (S)

f. Formulate, for approval by the DCI, standards for protecting information processing equipment from technical penetration. (S)

d. Issue advisories and develop technical guidance to departments and agencies of the Intelligence Community concerning exploration methods and techniques used or projected by hostile intelligence services, and recommend countermeasures to be used against penetration efforts.

e. "Provide training and educational guidance....." RATIONALE: Unclear what "instructional expertise" means. We view our role not as providing instructors but providing information and guidance to the existing training structure.

(para 5e of the DCI draft has been changed to clarify the need for instructors as well as information.)

g. Report all finds of technical penetrations promptly to the DCI Security Committee's Technical Surveillance Countermeasures Subcommittee (TSCS). In accordance with DCI policy, the TSCS will coordinate the testing and analysis of penetration devices among appropriate Intelligence Community facilities and will disseminate reporting and guidance to technical security components. (S)

h. Examine information processing equipment for potential technical penetration, conduct testing and analysis of penetrations of information processing equipment and provide to the TSCS appropriate reporting for guidance of technical surveillance countermeasures operations. (S)

5. To ensure full and timely consideration of active counterintelligence options against hostile penetrations, the team will report significant findings from the field by a secure, rapid means in compliance with DCI Procedural Guide 1, 2, and 3. The interagency evaluation teams will refer all finds of technical penetrations to the DCI Security Committee for designation of a department or agency to conduct an in-depth examination and report to the Community.

g. Replace as follows: Examine information processing equipment and their environs for potential technical penetration and disseminate appropriate reporting for guidance of technical countermeasures operations. Conduct indepth examinations of returned information processing, data handling, and associated hardware. Do indepth analysis and reporting to the Community of any information processing equipment penetration.

h. Replace as follows: Refer all finds of audio technical penetrations to the DCI Security Committee's Technical Surveillance Countermeasures Subcommittee for indepth examination and reporting to the Community.

RATIONALE: Conflicts with D/DCI guidance at meeting on 26 July 1985. D/DCI agreed that

i. In coordination with the existing CIA and Department of State programs for R&D on electronic intelligence penetration, conduct additional research and development programs to further the state of the art and to anticipate hostile advancements in that field. (S)

6. Heads of departments and agencies are responsible for establishing and maintaining measures to secure sensitive information at US facilities abroad under their authority. Heads of departments and agencies shall: (C)

a. Have full responsibility for conducting the security programs of their respective organizations, including physical, technical, personnel, and information security. (C)

4. e. In coordination with the State/CIA research and analysis laboratory, recommend R&D initiatives and evaluate ongoing projects to further the state of art and to anticipate hostile advancements in that field.

NSA would conduct all pre-find examinations of equipment and turn over audio penetration finds to the TSCS but NSA would conduct analysis and reporting, and preserve the option to use sensitive electronic devices for other offensive operations.

b. Provide pertinent information on intelligence, counterintelligence and security for use by the interdepartmental evaluation teams. (C)

c. Make available technically qualified personnel to participate in the interdepartmental evaluation teams. Requirements for staffing will be proposed by the DIRNSA and approved by the DCI and the Secretary of State. (C)

d. Refer all finds of technical penetrations promptly to the TSCS for coordination of testing and analysis and dissemination of reporting and guidance to technical security components. (C)

c. Delete second sentence. RATIONALE: Provided for in the document. Unnecessary restrictive and redundant to earlier language in the NSDD. Both DCI and SEC State approval are given for the operations and DIRNSA is charged with assembling the right kinds of experts.

7. Because of operational considerations bearing upon the protection of intelligence sources and methods, the Central Intelligence Agency will retain technical security responsibility for its stations and bases overseas. (S)	6. In those operational instances affecting the protection of sensitive sources and methods, the Assistant to the President for Security Affairs will determine the technical security responsibility for stations and bases overseas.	7. Delete phrase "and will not be subject to inspection by other organizations." Suggested rewrite. "Because of operational considerations bearing upon the protection of intelligence sources and methods, the Central Intelligence Agency will retain full control over all records and information in its locations and bases overseas." RATIONALE: D/DCI in the 25 July meeting agreed language could be interpreted to exclude teams from looking for electronic penetrations of CIA stations and bases. He further stated that his concern was to preserve the integrity of sources and methods at the stations and we interpreted this to mean he did not want the teams to have acccess to any sensitive records or information at the stations but that he did endorse the team looking for possible electronic penetrations by hostile intelligence agencies in and around the station.

Evaluation Priorities

8. The evaluation of facilities shall be carried out in the following priority: official US facilities in the Soviet Union; in other Warsaw Pact countries; in third world Soviet allied nations; and in other nations which are unable or unwilling to detect, deter, and prevent hostile intelligence services from penetrating official US facilities. (S)

See paragraph 4, above.

Relationship to Existing and Proposed Security Reviews, Policies, and Activities

9. The policies and activities established in this Directive are intended to supplement ongoing and proposed security policies and activities of the US Government (e.g., the Secretary of State's Advisory Panel on Overseas Security, the Director of Central Intelligence Security Committee and its Technical Surveillance Countermeasures Subcommittee). The

heads of all departments and agencies of the government, however, are directed to support the purposes and efforts established by this Directive. (U)

10. Nothing in this directive alters existing program, budget or operational control authorities of department or agency heads. (U)

11. Definitions

25X1

b. An official US facility abroad shall be defined to include an embassy, consulate, diplomatic residence, embassy or

consular compound, or other office space separate from the above but occupied by official US representatives. (U)

c. Interdepartmental evaluation teams are units created to conduct special evaluations of the security of sensitive information in US facilities abroad. They differ from other evaluation units in that they include experts in offensive intelligence operations. These experts are well versed in the techniques that the US uses to collect sensitive information from foreign installations. Defensive experts are included in these teams to insure a balanced look at security. (S)

D/ICS-85-7651, NSDD on Evaluating the Protection of Sensitive Information at Official United States Facilities Abroad (C)

STAT Prepared by: SECOM/ [redacted] /9 August 1985

Distribution:
Orig - Addressee, w/atts
1 - AD/ICS, w/atts
STAT 1 - EA/DDCI, [redacted] w/atts
1 - SECOM Chrono, w/atts
1 - SECOM Subject, w/atts
1 - ICS Registry, w/atts

Approved For Release 2007/11/01 : CIA-RDP87B01034R000600020005-3